Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional) 0378-0386P

Application Number	Filed
10/084,181-Conf. #004914	February 28, 2002
First Named Inventor: Akiko KUWAYAMA	
Art Unit: 2615	Examiner: A. J. Daniels

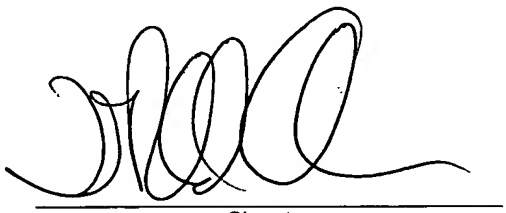
Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant /inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [ ] attorney or agent of record. Registration number _____
- [x] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. 40,439



Signature

D. Richard Anderson
Typed or printed name

(703) 205-8000
Telephone number

June 26, 2006
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

- [ ] *Total of 1 forms are submitted.

Attorney Docket: 0378-0386P

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	A. Kuwayama	Conf.: 4914
Appl No.:	10/084,181	Art Unit: 2615
Filed:	February 28, 2002	Examiner: A. Daniels
For:	DIGITAL CAMERA WITH A PERSONAL IDENTIFICATION	

REQUEST FOR PRE-APPEAL BRIEF CONFERENCE

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

June 26, 2006

Sir:

Applicant respectfully requests a review of the rejections in the Final Office Action dated January 24, 2006 (referred to as the Final Office Action) in the above-identified application. No amendments are being filed with this request.

This request is being filed concurrently with a Notice of Appeal.

The review is requested for the reasons set forth on the attached sheets.

REMARKS

The Examiner commits clear errors in rejecting claims 1-13, 17-19 and 23-28 in the Final Office Action.

The Examiner Fails to Establish a *Prima Facie* Case of Anticipation

The Examiner commits clear errors in alleging claims 9, 13, 17-19, 23 and 26 to be anticipated by Steinberg et al. (U.S. Patent 6,433,818) and alleging claim 10 to be obvious over Steinberg. Claim 9 is independent and claim 10 depends from claim 9, and claim 13 is independent and claims 17-19, 23 and 26 depend from claim 13.

Steinberg is directed toward a use of biometric data to eliminate unauthorized use of a camera and to deter camera theft. The Examiner alleges that the biometric data of Steinberg is equivalent to the fingerprint data as recited in the claims. In Steinberg, the process of setting up the biometric data is illustrated in Figure 8. To start the process, a user enters a predetermined password to instruct the camera to create the biometric data in Step 124. Afterwards, the user places either his eye to the view finder or his finger to the shutter button in Step 126, the camera records the biometric data in Step 128, and the biometric data is stored in Step 130. *See also Column 5, line 55 – Column 6, line 15.* As disclosed in Steinberg, the biometric signature data setup is performed regardless of whether or not there is preexisting biometric signature data.

In contrast, independent claim 9 requires a check to be made to determine if the inputted fingerprint data is identical with an already registered fingerprint data. If the inputted fingerprint data does not already exist, then the data is registered. In other words, there is a positive step of determining whether it is necessary to register the inputted fingerprint data. Steinberg discloses no such positive determination.

The Examiner relies upon column 6, lines 10-15 of Steinberg to allegedly disclose the feature of "checking if the inputted fingerprint data is identical with fingerprint data registered with a fingerprint register of the digital camera." *See Final Office Action, page 4, item 3, second paragraph.* This portion merely indicates that after the biometrics data is taken, the data is subsequently available for comparison purposes so that unauthorized access can be prevented. But the setup process itself does not check whether or not the biometrics data is preexisting or not.

The Examiner also alleges that the feature of "automatically initiating a registering of the inputted fingerprint data having a corresponding identifier with the fingerprint register in case no fingerprint data

is registered with the fingerprint register" is inherent and asserts that a database would have to be created in order for the camera to operate. However, the recited feature requires that the registering of the fingerprint data be initiated. The feature does not require that a database be created. Thus, the Examiner's inherency assertion does not apply which is a clear error.

In the Response to Arguments Section of the Final Office Action, the Examiner alleges that accepting of the password by the camera is viewed as the actual initiation because the accepting of the password precedes the placing of the finger of the shutter button. However, even the Examiner's assertion does not negate the fact that in Steinberg, setting up biometric data is in no way dependent upon whether or not there are preexisting biometric data. In short, the Examiner commits a clear error by failing to satisfy his burden under 35 U.S.C. §102 regarding independent claim 9.

Independent claim 13 recites, in part, "registering the fingerprint data of the user when it is determined that the digital camera is being used for the first time ever." Thus, claim 13 requires a determination of whether the digital camera is being used for the first time ever as a basis for registering the fingerprint data of the user. Steinberg cannot teach or suggest this feature.

The Examiner alleges that in Steinberg, the user entering a password and the password being accepted to setup the biometrics data is an indication that that the user is using the camera for the first time ever, i.e. the user has not used the camera before and wishes to enter his/her biometrics data. *See Final Office Action, pages 4-5.* In other words, the Examiner is alleging that setting up the biometrics data only occurs whenever the particular user handles the camera for the first time.

The Examiner's allegation fails on the following grounds. First, the Examiner is reading in language not present in the claim. The claim does not require that the registration occur when the digital camera is being used for the first time ever "by the user". The Examiner is required to give words of a claim their plain meaning unless defined in the specification. When the phrase "when the digital camera is being used for the first time ever" is given its plain meaning, it is clear that the claim requires the camera itself is being used for the first time. The Examiner commits a clear error by reading in the phrase "by the user" into the claim and by not giving words of the claim their plain meaning.

Further, even given the Examiner's unreasonable interpretation of claim 13, Steinberg still fails. The Examiner alleges that it is inherent that the only time the user starts the process of setting up the biometrics data as illustrated in Figure 8 is when he/she is using the camera for the first time. To establish inherency, the Examiner must demonstrate that the alleged characteristic necessarily flows from the teachings of the prior art. The fact that a certain result may occur is not sufficient to establish inherency.

In this instance, the Examiner only demonstrates that the camera may be used for the first time by the user when the biometrics data is setup. The Examiner does not demonstrate that the only time the biometrics data is setup is when the user uses the camera for the first time. It is entirely possible that a user can enter the biometric set up process illustrated in Figure 8 more than once, i.e. when his/her biometric data have previously been entered. The Examiner commits a clear error by failing to establish inherency of even his own unreasonable reading in of language not present in claim 13. In short, the Examiner made a clear error by failing to satisfy his burden under 35 U.S.C. §102 regarding independent claim 13.

The Examiner Fails to Establish a *Prima Facie* Case of Obviousness

The Examiner commits clear errors in alleging claims 1-2, 4-8, 11, 12, 24, 25 and 27 to be unpatentable over Steinberg in view of Wasula et al. (U.S. Publication 2002/0054224), alleging claim 3 to be unpatentable over Steinberg and Wasula and in further view of Kramer et al. (US Publication 2001/0043728), and alleging claim 28 to be unpatentable over Steinberg in view of Satoh (U.S. Publication 2001/0002933). Claims 1 is independent and claims 2, 4-8 and 27 depend from claim 1, claims 11 and 12 depend from independent claim 9, and claims 24 and 25 depend from independent claim 13.

As demonstrated above, the Examiner commits clear errors in rejecting independent claims 9 and 13 with reliance upon Steinberg. Wasula cannot rectify the Examiner's errors and thus, by extension, the Examiner commits clear errors in rejecting claims 11-12 and 24-25.

Independent claim 1 recites, in part, "an authorizer for storing therein an identifier specific to the fingerprint data identified by said comparison circuit" and "a controller for accessing said authorizer to reference the identifier stored in said authorizer and executing an instruction if the instruction is intended the handle a frame of image data associated with the identifier stored in said authorizer." The Examiner admits that Steinberg cannot teach or suggest these features. *See Final Office Action, page 8, lines 8-15.*

To allegedly correct these deficiencies of Steinberg, the Examiner relies upon Wasula. The Examiner alleges that the profiles as disclosed in Wasula are essentially the same as the identifier as recited in the claims. The Examiner alleges that Wasula teaches a digital camera for creating profiles for people with fingerprints. *See Final Office Action, page 8, last paragraph.* Again, the Examiner is reading in language not present in the claim. The claim recites that the identifier is specific to the fingerprint data. The language does not recite that the identifier is specific to a person. Thus, the Examiner commits a clear error.

In addition, the profiles as disclosed in Wasula are merely examples of a collection of instructions, i.e. macros, to be performed by the camera when it is desired to transfer images from the camera to a host computer. *See Applicant's Reply submitted on November 10, 2005, page 16, line 18 – page 17, line 11.* The customized profiles contain transferring instructions but there is no disclosure that the profiles are specific to a fingerprint data, let alone a person.

In response, the Examiner refers to Figure 3a of Wasula in which an exemplary name of the profile is "John Home Use". The Examiner alleges that a name of a collection of instructions in and of itself can be somehow identified with fingerprint data. This example merely indicates that the profiles may be given arbitrary names for the convenience of the user. The user in creating multiple profiles would likely name each profile to be readily identifiable. The name itself has no relevance whatsoever regarding whether it is identified with particular fingerprint data.

Also, Wasula doesn't even contemplate fingerprint data at all. The Examiner attempts to cover this clear error by tenuously linking the profile to a person and then to the fingerprint data since all persons have fingerprints.

In the Response to Arguments Section, the Examiner asserts that the profiles may be created by a user and access to the profiles may be denied to unauthorized users by employing a password for each profile and relies upon paragraph [0043] of Wasula. Thus, the Examiner alleges that because access to the user's profile by other users is denied through the password, the profile is particular to that user. And since the user has fingerprints, the profile is particular to the person's fingerprint data. Again, the Examiner is alleging inherency – namely that the feature of the identifier being specific to the fingerprint data is inherent – since the profile is locked for access only by the profile creator.

Paragraph [0043] states "a profile can be locked so that only the owner of the profile can upload images to the external device." This clearly leaves the option not locking the profile. When the profile is not locked, any user can access the unlocked profile. It is readily apparent that access to the profile may be denied, but not necessarily denied. Thus, the Examiner committed a clear error by failing to demonstrate inherency.

In short, the Examiner made a clear error by failing to satisfy his burden under 35 U.S.C. §103 regarding independent claim 1, and by extension, the dependent claims.

Conclusion

In summary, the Examiner committed clear error on several grounds as detailed above. Therefore, the rejections made in the Final Office Action should be withdrawn and the case allowed.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH &, BIRCH, LLP

Date: _____

By: _____
D. Richard Anderson
Reg. No. 40,439

DRA/HNS

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000